REMARKS

Claims 1 – 36 are present in the subject application.

In the Office Action dated May 25, 2005, the Examiner has rejected claims 16 - 19 under 35 U.S.C. §101 and has rejected claims 1 – 36 under 35 U.S.C. §103(a). Favorable reconsideration of the subject application is respectfully requested in view of the following remarks.

The Examiner has rejected claims 16 - 19 under 35 U.S.C. §101 as being directed toward non-statutory subject matter. The Examiner takes the position that these claims relate merely to a carrier signal that is not tied to a technological art, environment, or machine that would result in a practical application producing a concrete, useful, and tangible result.

This rejection is respectfully traversed. Initially, claims 16 – 19 are directed toward a carrier signal having computer program logic embedded therein for facilitating secure communications over a network. Thus, the claims are clearly directed toward a technological art (e.g., secure network communications) providing a concrete, useful, and tangible result. Further, the Examiner's attention is respectfully directed to the Examination Guidelines for Computer Related Inventions, dated March 28, 1996 and available at the USPTO web site. These guidelines include an automated manufacturing plant example including a claim directed toward a computer data signal embodied in a carrier wave (See claim 13). The guidelines indicate that this type of claim contains statutory subject matter. Copies of the relevant portions of the Examination Guidelines are submitted herewith for the Examiner's convenience and review. Accordingly, claims 16 – 19 are considered to be directed toward statutory subject matter.

The Examiner has rejected claims 1 – 9, 11 – 28 and 30 – 36 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,484,263 (Liu), further in view of U.S. Patent No. 6,601,762 (Piotrowski), and further in view of U.S. Patent No. 6,266,418 (Carter et al.). The Examiner takes the position that the Liu patent discloses all the features within these claims except for the information being stored remotely and negotiating parameters for a secure session. The Examiner further alleges that the Piotrowski and Carter et al. patents respectively teach these features and that it would have been obvious to combine the teachings of the Liu, Piotrowski, and Carter et al. patents to attain the claimed invention.

This rejection is respectfully traversed. Initially, the subject application has a filing date of December 8, 2000. However, the Piotrowski patent has an issue date of August 5, 2003 and a filing date of June 15, 2001. There is no apparent priority claimed by the Piotrowski patent to an earlier date. Since the earliest effective date of the Piotrowski patent (i.e., June 15, 2001) is **AFTER** the filing date of the subject application, the Piotrowski patent may not be utilized against the subject application. Accordingly, the rejection cannot stand.

In addition, the Liu and Carter et al. patents, do not disclose, teach, or suggest, either alone or in combination, the features recited in independent claims 1, 12, 16, 20, 31, and 34. Initially, an overview of the present invention is provided in order to assist in an understanding of the invention. Generally, a user may access a network or the Internet by a computer system or by placing a call to a voice browser system. The computer system typically stores locally security information (e.g., keys, certificates, etc.) for the user to negotiate parameters with a secure web site and establish a secure session. However, when the user accesses the network by telephone, voice browser systems do not store or have access to the user security information to

establish a secure session with a secure web site. Thus, conventional voice browser systems are unable to negotiate security parameters with secure web sites, thereby preventing user access to and secure sessions or communications with those sites.

The present invention overcomes this problem and enables voice browsers to negotiate security parameters and conduct a secure session with secure web sites for users. In particular, the present invention is directed toward a system for facilitating secure network communications including a security computer system utilized in conjunction with a voice browser residing on a server system. The present invention includes a module for a voice browser that creates a secure connection to the security system. The user provides an identification to the voice browser system that is transferred to and verified by the security system. Once the identification is verified, the user is prompted by the voice browser system to speak a phrase for voice verification. The verification speech signals are transferred from the voice browser system to the security system to verify those speech signals against speech signals of a particular authorized user associated with the identification and stored in a database. When the user is verified, the security system retrieves a user private key and certificate from the database. In response to the user subsequently accessing a web site residing on a secure server, the secure server and voice browser system initiate a secure key exchange. Data packets containing security information are identified by the voice browser system and transferred to the security system for processing, while security information from the security system is transferred to the secure server via the voice browser system. The resulting session key is securely transferred to the voice browser system to facilitate secure communications between the voice browser system and secure server. In other words, the security system handles processing of the security information from the

secure web site to enable the voice browser to conduct a secure session or provide secure communications with that site.

Accordingly, independent claims 1, 12, 16 and 20 recite the features of: a security module identifying security related information received by a network interface from a secure web site in response to a voice browser accessing that site based on voice commands from a user, wherein the security related information includes information enabling a secure session with a secure web site; voice and security information associated with authorized users and remotely stored from the network interface with the security information including information enabling negotiation of parameters for secure sessions with secure web sites; and a security system or secure communications module to process the security information identified by the security module for the network interface, to verify a user as an authorized system user based on a comparison of user voice signals with stored voice information, to retrieve security information of the verified user from remote storage, and to negotiate communication parameters with the secure web site utilizing the retrieved security information to facilitate the secure session between that site and the voice browser.

Independent claims 31 and 34 recite the features of: verifying the user as an authorized user based on a comparison of user voice signals with stored voice information of authorized users; retrieving security information of a verified user, including information enabling secure sessions with secure web sites, remotely stored from the network interface; and negotiating communication parameters for a voice browser or network interface with a secure web site accessed by the voice browser utilizing the retrieved security information to facilitate a secure

session between that site and the voice browser in response to the voice browser accessing the secure web site based on voice commands from the user.

The Liu patent does not disclose, teach or suggest these features. Rather, the Liu patent discloses a system and method for accessing password protected web sites through web browsers without manually supplying a user name and password by users. A browser maintains, for each user, one user security profile which stores the URLs and the corresponding log-in user name and password. When the browser receives a user name-password challenge from a web server, the browser first searches the user security profile for the URL the challenge is received from. If a match is found, the browser sends the challenging web server the user name and password that is associated with the matched URL (e.g. See Abstract).

Thus, the Liu patent discloses a browser providing a locally stored user name and password to access a password protected web site (e.g., See Fig. 2 and Column 3, lines 48 - 52). There is no disclosure, teaching, or suggestion of: verifying a user by comparing user voice signals with stored voice information of authorized users; the browser identifying security information from a secure web site for transfer to a security system; or a security system or negotiation unit to negotiate security parameters for the browser to conduct a secure session with a secure web site as recited in the independent claims. In fact, the disclosure of the Liu patent is limited to password access sites and is generally silent with respect to other forms of user verification, negotiation of security parameters and conducting secure sessions with web sites. Further, the Liu patent discloses storage of a URL, user name, and password locally within the browser, whereas the claims recite remote storage of security information enabling negotiation of communication parameters for the network interface to establish a secure session.

The Carter et al. patent does not compensate for the deficiencies of the Liu patent and similarly does not disclose, teach or suggest the above discussed features. Rather, the Carter et al. patent is directed toward an encryption device for a telephone having a handset and a base unit. The device includes a handset interface, a first converter, an encryption processor, a second converter, and a host interface. The handset interface receives analog output signals from the handset. The first converter converts the analog output signals into digital output signals. The encryption processor includes a compressor, a key manager, an encryptor, and a modulator. The key manager generates key material for encrypting the digital output signals. The compressor compresses the digital output signals, the encryptor encrypts the digital output signals based on the key material, and the modulator modulates the encrypted digital output signals. The second converter converts the encrypted digital output signals into encrypted analog output signals. The host interface receives encrypted analog output signals from the encryption processor and forwards the encrypted analog output signals to the base unit (e.g., See Abstract). The Carter et al. device is basically directed toward a device that can be connected between the handset and base unit of any of a variety of ordinary telephones to provide secure, full-duplex telephone conversations that are immune from eavesdropping with no degradation in speech quality (e.g., See Column 1, lines 51 – 55).

Thus, the Carter et al. patent discloses secure communications between telephones. There is no disclosure, teaching, or suggestion of: a secure session between a voice responsive network interface and a secure web site or, for that matter, verifying a user as an authorized user based on a comparison of user voice signals with stored voice information of authorized users; remotely storing user security information from the network interface; and a security system or negotiation unit negotiating communication parameters with a secure web site for the network

interface to enable a secure session between a secure web site and voice browser as recited in the independent claims. Accordingly, independent claims 1, 12, 16, 20, 31, and 34 are considered to overcome the Liu, Piotrowski, and Carter et al. patents and be in condition for allowance.

Dependent claims 2 – 9, 11, 13 – 15, 17 – 19, 21 – 28, 30, 32 – 33 and 35 – 36 depend, either directly or indirectly, from independent claims 1, 12, 16, 20, 31 or 34 and, therefore, include all limitations of their parent claims. These claims are considered to overcome the Liu, Piotrowski and Carter et al. patents and be in condition for allowance for substantially the same reasons as discussed above in relation to their parent claims and for further limitations recited in the dependent claims.

The Examiner has rejected claims 10 and 29 under 35 U.S.C. §103(a) as being unpatentable over the combination of the Liu, Piotrowski, and Carter et al. patents and further in view of U.S. Patent No. 5,341,426 (Barney et al.). The Examiner takes the position that the combination of the Liu, Piotrowski, and Carter et al. patents discloses all of the features within these claims except for stored security information including private keys and certificates of authorized system users. The Examiner further alleges that the Barney et al. patent discloses these features and that it would have been obvious to combine the Liu, Piotrowski, Carter et al., and Barney et al. patents to attain the claimed invention.

This rejection is respectfully traversed since the Piotrowski patent includes an effective date **AFTER** the filing date of the subject application as discussed above. Accordingly, since the Piotrowski patent cannot be utilized against the subject application, the rejection cannot stand.

In addition, claims 10 and 29 respectively depend, either directly or indirectly, from independent claims 1 and 20 and, therefore, include all of the limitations of their parent claims. As discussed above, the Liu and Carter et al. patents do not disclose, teach or suggest the features within independent claims 1 and 20. The Barney et al. patent does not compensate for the deficiencies of the Liu and Carter et al. patents. Rather, the Barney et al. patent is merely utilized by the Examiner to show use of private keys and certificates. Accordingly, claims 10 and 29 are considered to overcome the Liu, Piotrowski, Carter et al., and Barney et al. patents and be in condition for allowance.

In addition to the foregoing, there is no apparent reason or motivation to combine the teachings of the Liu, Carter et al., and Barney et al. patents. The Liu patent is directed toward access to password protected web sites without entry of the passwords. The Carter et al. patent is directed toward secure communication over telephones, while the Barney et al. patent discloses use of keys and certificates for secure connections as described above. Thus, the patents are directed toward diverging applications and there is no apparent reason, motivation or suggestion to combine their teachings absent prohibited hindsight derived from Applicant's own disclosure. Accordingly, the proposed combinations of the Liu, Carter et al., and Barney et al. patents do not render the claimed invention obvious.

The application, having been shown to overcome the issues raised in the Office Action, is considered to be in condition for allowance and a Notice of Allowance is earnestly solicited.

Respectfully submitted,

Stuart B. Shapiro

Stuart B. Shapiro
Registration No. 40,169

EDELL, SHAPIRO & FINNAN, LLC
1901 Research Boulevard, Suite 400
Rockville, Maryland 20850-3164
(301) 424-3640

Hand Delivered: 7/26/2005

Claim 13

A computer data signal embodied in a carrier wave comprising:

a. a compression source code segment comprising . . . [recites self-documenting source code]; and

b. an encryption source code segment comprising . . . [recites self-documenting source code].

EXAMINATION GUIDELINES FOR COMPUTER-RELATED INVENTIONS
Example: AUTOMATED MANUFACTURING PLANT

Table for Claim 13

BOX 2	Q.2a. Does disclosed invention have practical application?	YES	GoTo: Q.2b	Note 1
	Q.2b. Is disclosed invention in technological arts?	YES	GoTo: Q.6a	Note 2
BOX 6	Q.6a. Is claimed invention a computer program *per se*?	NO	GoTo: Q.6b	Note 3
	Q.6b. Is claimed invention a data structure *per se*?	NO	GoTo: Q.6c	
	Q.6c. Is claimed invention non-functional descriptive material?	NO	GoTo: Q.6d	
	Q.6d. Is claimed invention a natural phenomenon?	NO	GoTo: Q.8	Note 4
BOX 8	Q.8. Is claimed invention a series of steps to be performed on a computer?	NO	GoTo: Q.9	
BOX 9	Q.9. Is claimed invention a product for performing a process?	YES	GoTo: Q.10	
BOX 10	Q.10. Is claimed invention a specific machine or manufacture?	YES	GoTo: END	Note 5
BOX 12	Q.12a. Does process have post-computer process activity?		GoTo:	
	Q.12b. Does process have pre-computer process activity?		GoTo:	
BOX 13	Q.13a. Does process manipulate abstract idea w/o limitation to a practical application?		GoTo:	
	Q.13b. Does process solve math problem w/o limitation to a practical application?		GoTo:	

Table Notes for Claim 13

Note 1: Disclosed invention monitors and controls an automated plant's manufacturing process.

Note 2: Disclosed invention uses a general purpose computer system.

Note 3: Claimed invention recites specific software embodied on a computer-readable medium, *i.e.*, specific software embodied in a carrier wave.

Note 4: Most likely, the "data signal" does not occur as a natural phenomenon. The Examiner bears the burden of establishing that a claimed invention is a natural phenomenon. Therefore, absent object evidence to support the position that the "data signal" is a natural phenomenon, such a position would be untenable.

Note 5: Claimed invention recites specific software. *See* Guidelines, Section IV.B.2(a)(ii). THE REMAINDER OF THE EXAMINATION MUST BE COMPLETED.

For a more detailed analysis of the claim, see Examination Guidelines for Computer Related Inventions, Example: Automated Manufacturing Plant Claim Analysis appended to these examples.

Claim 10 is further rejected under 35 U.S.C§ 103 as obvious. The embodiment of mere data on a "computer system apparatus" would have been obvious to a person of ordinary skill in the art at the time of invention.

CLAIM 11:

Claim 11 is unclear as to whether it claims a computeprogram *per se* or a computer program embodied on a computer-readable medium. In particular, the preamble phrase "computer program" defines a set of instructions for execution on a computer, *i.e.*, a computer program *per se*. The body of the claim, however, recites means plus function language which defines at least a set of instructions embodied on a computer-readable medium to perform the recited functions. The claim is rejected under 35U.S.C. § 112, ¶2 for failure to distinctly point out and claim the invention.

Claim 11 is also rejected under 35U.S.C. § 101. It is reasonable to presume that applicant seeks to claim a computer program *per se*. A computer program *per se* cannot define any structural and functional interrelationships that permit the computer program's functionality to be realized.

The following amendment to claim 11 would render claim 11 a statutory article of manufacture claim:

- embodying the computer program on a computer-readable medium.

Claim 11 could also be amended to recite a statutory process.

CLAIM 12:

Claim 12 is an article of manufacture claim. It recites a computer program with two claim limitations:

a. Element a. recites a specific source code segment for compression; and
b. Element b. recites a specific source code segment for encryption.

Reviewed as a whole, and given its broadest reasonable interpretation, the claim is limited to a specific article of manufacture. Also, the computer program is embodied on a computer-readable medium. Thus, claim 12 is a statutory article of manufacture claim.

CLAIM 13:

Claim 13 is an article of manufacture claim. It recites a computer program with two claim limitations:

a. Element a. recites a specific source code segment for compression; and
b. Element b. recites a specific source code segment for encryption.

Reviewed as a whole, and given its broadest reasonable interpretation, the claim is limited to a specific article of manufacture. Also, the computer program is embodied on a computer-readable medium--the carrier wave. Thus, claim 13 is a statutory article of manufacture claim.